IN THE CLAIMS

1. (Currently Amended) A method for providing access control in a computing system environment, the method comprising the steps of:

receiving an access request;

selecting, based on the access request, a ~~selected~~ set of rules containing at least one rule from a ~~at least one~~ master set of rules; and

~~performing at least one rule operation in the at least one rule in the selected set of rules to produce an access control decision until at least one of:~~

~~i) a rule operation including a disregard instruction is performed to limit performance of rule operations in the selected set of rules; and~~

~~ii) all rule operations in the selected set of rules that are applicable to the access control decision are performed;~~

~~wherein at least one rule in the selected set of rules contains a rule operation including an unconditional disregard instruction; and~~

~~wherein the step of performing includes the steps of:~~

producing an access control decision based on performing ~~less than all~~ rule operations in a given rule ~~defined within the at least one rule in~~ of the selected set of rules by sequentially performing rule operations in the given ~~each~~ rule until performing a ~~in the selected set of rules until the unconditional~~ disregard instruction ~~is performed~~, the disregard instruction including disregard criteria identifying a type of other rule operations in the selected set of rules to disregard from performing; and ~~thereby terminating the performance of any remaining rule operations in the selected set of rules~~

after performing the unconditional disregard instruction in the given rule:

i) evaluating the disregard criteria against any remaining unperformed rule operations in other rules of the selected set of rules, the other rules being rules other than the given rule;

ii) marking any remaining unperformed rule operations in the other rules of the selected set of rules that match the disregard criteria to be disregarded from further rule processing; and

iii) executing remaining unmarked rule operations in the other rules in the selected set of rules.

2. (Original) The method of claim 1 wherein the step of performing includes the step of producing an access control decision indicating whether to allow access, on behalf of a requestor submitting the access request, to an resource in the computing system environment.

3. (Currently Amended) The method of claim 1 wherein the step of selecting includes the steps of:

determining an identity of a ~~the~~ resource in the computing system environment to which access is requested in the access request; and

applying at least one filter operation, using the identity of the resource, for rules in the ~~at least one~~ master set of rules to produce the selected set of rules for use in determining the access control decision for ~~to~~ the resource.

4. (Currently Amended) The method of claim 3 further including the step of:

determining a role identity of a requestor submitting the access request; and

wherein the step of applying applies the at least one filter operation, using the role identity of the requestor submitting the access request in combination with the identity of the resource, for rules in the ~~at least one~~ master set of rules to produce the selected set of rules for use in determining the access control decision to the resource.

5. (Cancelled)

6. (Previously Presented) The method of claim 1 wherein the selected set of rules is arranged hierarchically such that rules containing rule operations that are more specific are performed before rule operations that are more general.

7. (Canceled)

8. (Canceled)

9. (Currently Amended) The method of claim 1 wherein the step of selecting includes the steps of:

determining an identity of a resource in the computing system environment to which access is requested in the access request; and

applying at least one filter operation, using the identity of the resource, for rules in the at least one master set of rules to produce the selected set of rules for use in determining the access control decision to the resource; and

wherein the method further includes the step of determining a role identity of a requestor submitting the access request; and

wherein the step of performing includes sequentially processing ~~processes~~ each rule operation in the selected set of rules using the role identity of the requestor submitting the access request in combination with the identity of the resource to determine if the requestor using the role identity can access the resource.

10. (Canceled)

11. (Canceled)

12. (Currently Amended) The method of claim 1 ~~claim 10~~ wherein:

the selected set of rules is arranged hierarchically such that rules containing rule operations that are more specific are performed before rules containing rule operations that are more general such that placement of the disregard instruction in one of the ~~at least one~~ rules in the selected set of rules causes the step of performing to control an amount of access control provided to

a ~~the~~ requestor that submitted the access request for access to a respective ~~the~~ resource.

13. (Currently Amended) The method of claim 1 ~~claim 10~~ wherein the disregard instruction is a conditional instruction that has a condition that must be met before the disregard instruction is performed.

14. (Original) The method of claim 1 wherein:

at least one rule in the selected set of rules contains a relation that defines a condition based on a group definition; and

wherein at least one of the steps of selecting and performing includes the step of:

performing the relation to determine if at least one of a requestor, an access, and a resource specified in the access request satisfy the condition based on the group definition.

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Canceled)

19. (Currently Amended) A computer system configured to provide access control, the computer system comprising:

at least one input/output interface;

a processor;

a memory system encoded with an authorization program;

at least one authorization database;

an interconnection mechanism coupling the processor, the at least one input/output interface, the memory system, and the at least one authorization database;

based at least in part on the processor executing the authorization program, the processor supporting steps of:

receiving an access request;

selecting, based on the access request, a set of rules containing at least one rule from a master set of rules;

producing an access control decision based on performing rule operations in a given rule of the selected set of rules by sequentially performing rule operations in the given rule until performing a disregard instruction, the disregard instruction including disregard criteria identifying a type of other rule operations in the selected set of rules to disregard from performing; and

after performing the unconditional disregard instruction in the given rule:

i) evaluating the disregard criteria against any remaining unperformed rule operations in other rules of the selected set of rules, the other rules being rules other than the given rule;

ii) marking any remaining unperformed rule operations in the other rules of the selected set of rules that match the disregard criteria to be disregarded from further rule processing; and

iii) executing remaining unmarked rule operations in the other rules in the selected set of rules.

~~wherein the at least one input/output interface receives an access request from a requestor and the processor performs the authorization program in the memory system to select, based on the access request, a selected set of rules containing at least one rule from at least one master set of rules maintained within the at least one authorization database; and~~

~~wherein the processor performs at least one rule operation in the at least one rule in the selected set of rules to produce an access control decision in the memory system until at least one of:~~

~~i) a rule operation including a disregard instruction is performed to limit performance of rule operations in the selected set of rules; and~~

~~ii) all rule operations in the selected set of rules that are applicable to the access control decision are performed;~~

~~wherein at least one rule in the selected set of rules in the authorization database contains a rule operation including an unconditional disregard instruction; and~~

~~wherein when the processor performs at least one rule operation, the processor performs less than all rule operations defined within the at least one rule in the selected set of rules by sequentially performing rule operations in each rule in the selected set of rules until the unconditional disregard instruction is performed thereby terminating the performance of any remaining rule operations in the selected set of rules.~~

20. (Currently Amended) The computer system of claim 19 wherein the processor, via performance of ~~the~~ at least one rule operation, produces an access control decision indicating whether to allow access, on behalf of a ~~the~~ requestor submitting the access request, to a ~~an~~ resource in the computing system environment.

21. (Currently Amended) The computer system of claim 19 wherein:

the processor performs the authorization program to select the ~~the selected~~ set of rules and to determine an identity of a resource in the computing system environment to which access is requested in the access request; and

the processor performs the authorization program to apply at least one filter operation from the at least one authorization database, using the identity of the resource, for rules in the ~~at least one~~ master set of rules to produce the selected set of rules for use in determining the access control decision to the resource.

22. (Currently Amended) The computer system of claim 21 ~~claim 19~~ wherein the processor performs the authorization program which determines a role identity of a requestor submitting the access request; and

wherein when the processor performs the authorization program to apply at least one filter operation, the authorization program applies the at least one filter operation, using the role identity of the requestor submitting the access request in combination with the identity of the resource, for rules in the ~~at least one~~ master set of rules to produce the selected set of rules for use in determining the access control decision to the resource.

23. (Cancelled)

24. (Previously Presented) The computer system of claim 19 wherein the selected set of rules is arranged hierarchically such that when the processor performs the authorization program, rules containing rule operations that are more specific are performed before rule operations that are more general.

25. (Canceled)

26. (Canceled)

27. (Original) The computer system of claim 19 wherein when the processor performs the authorization program to select a selected set of rules, the processor:

determines an identity of an resource to which access is requested in the access request; and

applies at least one filter operation, using the identity of the resource, for rules in the at least one master set of rules to produce the selected set of rules for use in determining the access control decision to the resource; and

wherein when the processor performs the authorization program, the processor determines a role identity of a requestor submitting the access request; and

wherein the processor sequentially processes each rule operation in the selected set of rules using the role identity of the requestor submitting the access request in combination with the identity of the resource to determine if the requestor using the role identity can access the resource.

28. (Original)

29. (Original)

30. (Currently Amended) The computer system of claim 19 ~~claim 28~~ wherein:

the selected set of rules is arranged hierarchically such that rules containing rule operations that are more specific are performed by the processor before rules containing rule operations that are more general such that placement of the disregard instruction in one of the at least one rules in the selected set of rules causes the authorization program, when performed on the processor, to control an amount of access control provided to the requestor that submitted the access request for access to the resource.

31. (Original) The computer system of claim 28 wherein the disregard instruction is a conditional instruction that has a condition that must be met during processing by the processor before the disregard instruction is performed.

32. (Original) The computer system of claim 19 wherein:

at least one rule in the selected set of rules contains a relation that defines a condition based on a group definition; and

wherein when the processor performs at least one of the operations of selecting and performing, the processor performing the relation to determine if at

least one of a requestor, an access, and a resource specified in the access request satisfy the condition based on the group definition.

33. (Canceled)

34. (Canceled)

35. (Canceled)

36. (Canceled)

37. (Canceled)

38. (Canceled)

39. (Canceled)

40. (Canceled)

41. (Canceled)

42. (Canceled)

43. (Canceled)

44. (Canceled)

45. (Currently Amended) A method for controlling applicability of rule operations in a rule-based access control system, the method comprising the step of:

selecting at least two rules ~~one rule~~ for performance to determine an access control decision, the at least two rules including a first rule and a second rule; ~~and~~

performing a rule operation in the first rule of the at least two rules ~~in the at least one rule~~, the rule operation including a disregard instruction that, when performed, causes non-performance of at least one ~~other~~ rule operation in the second rule ~~in at least one rule~~ that is disregarded based on the disregard instruction ~~selected for performance to determine the access control decision~~; and

performing at least one rule operation in the second rule other than the at least one rule operation in the second rule that is disregarded.

46. (Canceled)

47. (Canceled)

48. (Canceled)

49. (Canceled)

50. (Canceled)

51. (Canceled)

52. (Currently Amended) A method for providing access control in a computing system environment, the method comprising the steps of:

receiving an access request;

selecting, based on the access request, a set of rules containing multiple rules from at least one master set of rules, at least one of the multiple rules including multiple rule operations to be performed in sequential order;

for a ~~given~~ first rule of the multiple rules:

performing a filter operation associated with the ~~given~~ first rule to identify whether to execute any rule operations in the ~~given~~ first rule; and

performing multiple operations in the first rule to determine whether to provide access to a storage system in response to receiving the access request, the first rule including a disregard instruction that, when executed, limits performance to fewer than all rule operations in a second rule of the selected set of rules as specified by disregard criteria in the disregard instruction.

53. (Currently Amended) A method as in claim 52, wherein the filter operation is an IF-THEN operation and performance of the IF-THEN operation provides an indication whether to perform rule operations in the ~~given~~ first rule.

54. (Canceled)

55. (Currently Amended) A method as in claim 52 ~~claim 54~~, wherein the disregard instruction is a conditional disregard instruction, which limits a performance of other rule operations in multiple rules other than the ~~given~~ first rule in the selected set of rules depending on occurrence of a corresponding condition as specified by the disregard criteria in the disregard instruction.

56. (Currently Amended) A method as in claim 55 further comprising:

performing at least one other rule operation in the ~~given~~ first rule as well as other rules in the selected set of rules after performing the ~~a~~ conditional disregard instruction.

57. (Currently Amended) A method as in claim 53 ~~claim 52~~, wherein performance of the IF-THEN operation includes identifying whether an application generating the access request uses a particular resource in the

storage system as well as whether a requestor associated with the access request is a member of a particular specified group and, if so, performing the rule operations in the first ~~given~~ rule.

58. (New) A method for providing access control in a computing system environment, the method comprising:

receiving an access request;

in response to receiving the access request, selecting a set of rules for processing to determine whether to permit the access request;

during processing of the set of rules, performing a conditional disregard rule operation in the set of rules;

based on performing the conditional disregard rule operation, disregarding execution of at least one rule operation other than the conditional disregard rule operation in the set of rules as specified by the conditional disregard rule operation; and

after performing the conditional disregard rule operation, performing at least one other rule operation in the set of rules not specified by disregard criteria in the conditional disregard rule operation.

59. (New) A method as in claim 58 further comprising:

comparing disregard criteria in a data field associated with the conditional disregard rule operation to data in other rule operations to identify which other rule operations in the selected set of rules to disregard from performance.

60. (New) A method as in claim 58, wherein a field of data in the conditional disregard rule operation specifically identifies a first type of rule operations that are to be disregarded from execution in the set of rules, execution of the conditional disregard rule not having any affect on whether to perform a second type of rule operations in the set of rules.

61. (New) A method as in claim 60, wherein performing a conditional disregard rule operation further comprises identifying disregard criteria in the conditional disregard rule operation, the method further comprising:

upon performing the conditional disregard rule operation, marking any remaining unperformed rule operations in the set of rules as identified by the disregard criteria; and

continuing performance of rule operations in the set of rules that are not marked to be disregarded.

62. (New) A method as in claim 58 further comprising:

during processing of the set of rules, performing an unconditional disregard rule operation in the set of rules that results in termination of performing any other rule operations in the selected set of rules.

63. (New) A method for providing access control in a computing system environment, the method comprising:

receiving an access request;

in response to receiving the access request, selecting a first set of rules and a second set of rules for processing to determine whether to permit the access request, the first set of rules and the second set of rules each including multiple rule operations;

during processing of the first set of rules, performing a disregard rule operation in the first set of rules; and

based on performing the disregard rule operation, disregarding execution of at least one rule operation in the second set of rules as identified by the disregard rule operation.

64. (New) A method as in claim 63, wherein selecting the first set of rules and the second set of rules includes applying a respective first filter and a second

filter to identify whether to select the first set of rules and the second set of rules for execution.

65. (New) A method as in claim 63 further comprising:

after disregarding execution of at least one rule operation in the second set of rules as identified by the disregard rule operation in the first set of rules, performing at least one rule operation in the second set of rules not associated with the disregard rule operation.

66. (New) A method as in claim 63 further comprising:

following completion of executing the first set of rules and the second set of rules, generating an access control decision whether to permit the access request.

67. (New) A method as in claim 63, wherein the disregard rule operation is a conditional disregard rule operation, a field of data in the conditional disregard rule operation specifically identifying a first type of rule operations that are to be disregarded from execution in the first set of rules and the second set of rules, execution of the conditional disregard rule not having any affect on whether to perform a second type of rule operation in the second set of rules.

68. (New) A method as in claim 67, wherein performing a conditional disregard rule operation includes identifying disregard criteria in the conditional disregard rule operation, the method further comprising:

upon performing the conditional disregard rule operation, marking any remaining unperformed rule operations in the first set of rules and the second set of rules as identified by the disregard criteria; and

continuing performance of rule operations in the first set of rules and the second set of rules that are not marked to be disregarded.

69. (New) A method as in claim 67 further comprising:

during processing of the first set of rules, performing an unconditional disregard rule operation that results in termination of performing all other rule operations in the selected first set of rules and the second set of rules.

70. (New) A method for providing access control in a computing system environment, the method comprising:

receiving an access request to access data in the computing system environment;

comparing the access request to a master rule set, each rule in the master rule set including a filter and a corresponding set of rule operations to be performed pending evaluation of the filter condition; and

for each rule containing a filter operation that evaluates to indicate execution of rule operations of that rule, executing the rule operations of that rule;

during execution of rule operations of that rule, executing a first conditional disregard instruction that establishes a first set of pre-conditions that must be met in successive rules in the master rule set in order for those successive rules to be executed after the rule containing the first conditional disregard instruction has been executed; and

executing at least one successive rule in the master rule set for which the access request meets the filters of those successive rules, and for which the first set of pre-conditions established by executing the first conditional disregard instruction are also met.

71. (New) The method of claim 70 wherein executing only the successive rules in the master rule set comprises:

executing a second conditional disregard instruction that establish a second set of pre-conditions that must also be met in addition to the first set of pre-conditions established by the first disregard instruction for any remaining successive rules in the master rule set to be executed.

72. (New) The method of claim 71 wherein pre-conditions established by execution of the conditional disregard instructions indicate a type of data upon which rule operations of successive rules in the master rule set operate that are not to be executed during execution of the successive rules in the master rule set.

73. (New) The method of claim 72 wherein the filter of at least one rule in the master rule set includes a test of whether an application associated with the access request uses a particular resource associated with the request.

74. (New) The method of claim 72 wherein the filter of at least one rule in the master rule set includes a test of whether at least two resources associated with the access request are connected to each other.

75. (New) The method of claim 72 comprising skipping execution of those successive rules in the master rule set for which the access request does not meet the filters of those successive rules, and for which the first and second set of pre-conditions established by executing the first and second disregard instructions are not met.

76. (New) A computer program product having a computer-readable medium including computer program logic encoded thereon that when executed on a computer system provides a method for controlling access to a resource, and wherein when the computer program logic is executed on a processor in the computer system, the computer program logic causes the processor to perform the operations of:

receiving an access request to access data in the computing system environment;

comparing the access request to a master rule set, each rule in the master rule set including a filter and a corresponding set of rule operations to be performed pending evaluation of the filter condition; and

for each rule containing a filter operation that evaluates to indicate execution of rule operations of that rule, executing the rule operations of that rule;

during execution of rule operations of that rule, executing a first conditional disregard instruction that establishes a first set of pre-conditions that must be met in successive rules in the master rule set in order for those successive rules to be executed after the rule containing the first conditional disregard instruction has been executed; and

executing at least one successive rule in the master rule set for which the access request meets the filters of those successive rules, and for which the first set of pre-conditions established by executing the first conditional disregard instruction are also met.